

# Preparing Your Phone for a Trusted Helper

Friendly guide for seniors & caregivers  
regarding their tech devices and accounts

# Welcome & Class Overview



- The importance of setting up phones
- Android/ iPhone
- The importance of setting up an account inventory
- Managing passwords

# Your Digital Life Is Bigger Than You Think

## How Many Apps do you have?



# Why This Matters: Loss of Access

- Loss of Money
- Loss of Memories
- Loss of Access to 2FA
- Identity theft
- False use of NIL



# Choosing a digital executor

## Tips for Choosing a Trusted Contact

- **Trust:** Choose someone you trust completely, as they will have access to your personal information.
- **Tech-Savvy:** It's helpful to choose someone who is comfortable with technology.
- **Communication:** Discuss your plans with your trusted contact so they know what to do if the time comes.

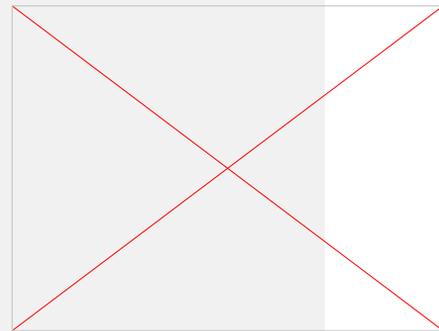
# Preparing to Share Access Safely

- There are many ways you can share access
- Password Managers: [Emergency Contacts](#)
- Paper & Pen Lists
- Excel Lists
- Biometric Data considerations
- Back up systems
- 2 FA/MFA limitations

# Android: Device-Level Access

## Android Devices/Google Accounts

1. Sign in to your Google account
2. Click on your profile picture in the top-right corner of the screen
3. Click on "Manage your Google Account"
4. Click on "Data & privacy" from the menu
5. Scroll down to "More options"
6. Click "Make a plan for your digital legacy"
7. Click on "Start" under "Inactive Account Manager"
8. Follow the prompts to choose your legacy contact and set your preferences.



# Android: Setting Up a Trusted Contact

Here's how you can prepare your Android phone to ensure your loved ones can access your important information:

1. **Set Up Screen Lock and Share with Trusted Person:** Make sure you have a screen lock set up on your phone (PIN, password, or pattern) and share this information with someone you trust completely.
2. **Backup Your Data:** Regularly back up your data to a cloud service like Google Drive. This ensures that your information is stored securely and can be accessed from another device if needed.
  - **Go to Settings > System > Backup > Back up to Google Drive** and ensure this is turned on.
3. **Enable Account Recovery Options:** Set up account recovery options to make it easier for your loved ones to access your Google account.
  - **Go to your Google Account > Security > Ways we can verify it's you > Recovery email and Recovery phone.**
4. **Use a Password Manager:** A password manager can store all your account passwords in one place. Share the master password with your trusted contact.
  - Popular options include LastPass, 1Password, and Google's built-in password manager.
5. **Grant Access to Google Account:** You can add a trusted contact to your Google account who can access it if needed.
  - **Go to your Google Account > People & sharing > Grant access to your account > Add a trusted person's email.**

# iPhone: Setting Up Legacy Contact

## Apple iPhone

1. Go to Settings, then tap your name
2. Tap Sign-In & Security, then tap Legacy Contact
3. Tap Add Legacy Contact (typically someone who is already an existing contact in your phone). You may have to authenticate via Face ID, passcode, or Touch ID.
4. Once added, you can share your 'access key' with your legacy contact, usually through a text message. If something were to happen to you, they would need this and a copy of your death certificate to request access.

More info: [How to add a Legacy Contact for your Apple Account - Apple Support](#)

*You can add a legacy contact to your Mac devices as well.*

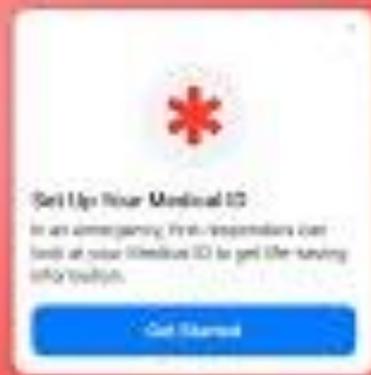
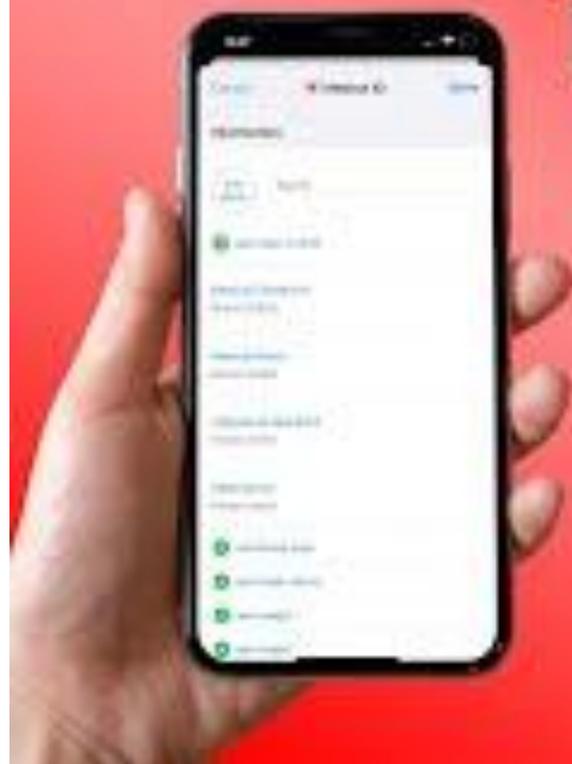


MEDICAL ID



**How to Set an Emergency Contact on iPhone (and Why)**

# HOW TO SETUP \*Medical ID ON YOUR iPhone



# Theft Protection & Location Lock

The "theft mode" feature is called **Stolen Device Protection** and is available on the latest versions of iOS, including **iOS 17.3 and newer**. To enable it, go to **Settings > Face ID & Passcode** (or **Touch ID & Passcode**), enter your passcode, and then tap on **Stolen Device Protection** to turn it on. This feature adds an extra layer of security,



# Inventory Your Accounts

## 1. Payments

- Banks
- Money Apps
- Brokerage/Trading Accounts
- Insurance
- Gambling Accounts
- Rental Income Platforms

## 2. Blockchain, Cryptocurrencies, Exchanges, Tokens and Web 3.0

- Blockchain Information
- Tokenized Assets on Blockchain
- NFT's ( Non-Fungible Tokens)
- Crypto Exchanges
- Crypto Wallets

## 3. Biodata & Health

- Medical Records
- Frozen bio-specimens
- DNA and genealogy mapping

## 4. Travel and Loyalty

- Airline points
- Hotel points
- Cruise lines

## 5. Social Media, Emails, Dating Photo & Video Storages, Blogs & Vlogs, Intellectual Properties

- Emails
- Dating
- Photo & Video Storage
- Blogs & Vlogs
- Website Domain Names

## 6. Telephone, Web Services, Utilities, TV Streaming, Gaming Services, Phone Devices

- Phone Carriers
- Streaming Services
- Internet Service Providers
- Gaming Platforms

## 7. Shopping & Ecommerce

- Income Platforms
- Crowdfunding
- Large Box Membership Stores

# Social Media Legacy Options



Tiffany Wang-Lawdanowski · 1st

Senior Counsel at Antelith  
Antelith · Northcentral University  
Phoenix, Arizona Area · 341 connections



Tiffany Wang-Lawdanowski · 1st

**In remembrance**

Senior Counsel at Antelith  
Antelith · Northcentral University  
Phoenix, Arizona Area · 341 connections

# Financial & Email Accounts

- Banking Accounts
- Brokerage Accounts
- Cryptocurrency Accounts
- Gambling Accounts
- Hobby/ trading accounts
- Side Hustling business accounts
- Emails

# Devices & Cloud Storage

- iCloud
- Drop Box- Subscription!
  - Does Dropbox delete files after inactivity? If you've been notified over email that your account is inactive, and you don't take any steps to keep your account active, your account will be automatically closed and your files will be deleted within 90 days
- Storage Vaults -Subscription!

# Password Managers & Sharing Safely

- We may have passwords in many places, as well as passkeys
- Take a video of yourself
- Take a screen recording
- [USB Credit Cards](#)



# Review: Your Care Access Checklist

- **Care Access Checklist for Your Digital Executor**

- *(Who should have access to what)*

- **1. Emergency Contacts**

- Trusted family member knows location of passwords or password manager
- Caretaker has access to phone passcode (or backup unlock method)

- **2. Financial & Legal**

- Executor or financial advisor has access to:
  - Online banking and bill pay accounts
  - Investment, insurance, and pension portals
  - Estate documents or trust folder

- **3. Health & Medical**

- Caregiver or family contact can access:
  - Patient portals (MyChart, etc.)
  - Prescription refills
  - Health insurance accounts



- **4. Devices & Cloud**

- Someone has access to:
  - Phone, tablet, and computer login codes
  - Cloud storage (Google Drive, iCloud, Dropbox)

- **5. Communication & Social**

- Family contact can manage:
  - Email and voicemail
  - Social media or messaging apps (optional)

- **6. Utilities & Subscriptions**

- Executor can view or cancel:
  - Internet, phone, TV, streaming, memberships

A spiral-bound notebook with a black cover and silver wire binding is centered in the frame. The notebook's pages are white, and the words "THANK YOU" and "VETERANS" are printed in a bold, blue, serif font, one above the other. The notebook is placed on a light-colored wooden surface. To the left, the blue field of an American flag with white stars is visible. To the right, the red and white stripes of the flag are visible. The background wall is a light, textured surface.

**THANK YOU  
VETERANS**

# Thank You & Next Steps

Free  
Access Care  
Guide Here:



<https://dexitplan.aflip.in/8f46c7250a.html>